Cybercrime is evolving due to a combination of several key factors: high financial profitability, the rapid development of technology and the growth of computerization of society, as well as the low level of awareness of many users.

References:

1. Marleen Weulen Kranenbarg, Jean-Louis van Gelder, Ard J. Barends, Reinout E. de Vries. 2023. “Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets.” // Computers in Human Behavior. Volume 140. March 2023. https://doi.org/10.1016/j.chb.2022.107576 .

2. Межа між кіберзлочинністю та етичним хакінгом — 15 типів хакерів, які вам потрібно знати у 2023 році [Electronic resource]. URL: https://10guards.com/ua/blog/2023/06/20/the-thin-line-between-cybercrime-and-ethical-hacking-the-15-types-of-hackers-you-need-to-know-in-2023/ (date of application 10.10.2025).

3. Truong Jack Luu, Binny M. Samuel, Michael Jones, J.C. Barnes. 2025. “Exploring how the Dark Triad shapes cybercrime responses” // Personality and Individual Differences. Volume 244. October 2025. https://doi.org/10.1016/j.paid.2025.113250 .

Жицька Валерія Олегівна
Студентка н.гр. 117 СПД ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

СТАН ТА ШЛЯХИ ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

В наш час особливо, під час воєнного стану в Україні, дуже важливим є кібербезпека громадян і країни в цілому. Тому в роботі було розглянуто деякі проблеми кібербезпеки в Україні і шляхи їх усунення. Було проаналізовано проблеми в процесі створення безпечного кіберпростору в Україні, встановлено, що одним із можливих шляхів до створення безпечного кіберпростору є розвиток відповідної освіти в Україні.

Громадяни мають бути забезпечені знаннями щодо захисту особистих даних, продуктів власної творчості, ділової інформації та мати відповідні вміння щодо безпечного використання інформаційного середовища. Доведено важливість поширення комп'ютерної грамотності серед студентів.

Сучасні інформаційні технології розвиваються швидко. Одночасно і зростає рівень незахищеності людини в інфопросторі, який став невід'ємною частиною життя.

Кіберзагрози та кібератаки стали звичайним явищем в сучасному світі. Кібербезпека – частина національної безпеки. Її стан – умова стабільного розвитку країни. Тому постійне вдосконалення системи кіберзахисту – одна із актуальних сучасних завдань держави. Шляхів такого вдосконалення існує достатньо. Важливою є міжнародна співпраця в обміні досвідом між різними країнами світу стосовно створення безпечного кіберпростору. В умовах посилення кібератак та інформаційної війни для України така співпраця є необхідною, а робота зі створення ефективної системи кіберзахисту має проходити пришвидшеними темпами, особливо під час воєнного стану в країні.

Вважається, що кіберпростір дуже скоро стане новим полем для війн в сучасному світі, а рівень обороноздатності країни буде визначатись за показниками якості та ефективності кіберзахисту. Тому дуже важливо знайти оптимальні шляхи удосконалення системи кібербезпеки в Україні та забезпечити їх впровадження.

Вперше поняття «кіберпростір» було використано у 1980-х роках. *Кіберпростір* – це нове середовище, яке з'явилося внаслідок функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем; нова сфера, яка не існує в фізичній формі, але передбачає активну взаємодію осіб, програмного забезпечення та послуг у мережі Інтернет.

Кібербезпека – це захищеність важливих інтересів людини, суспільства і держави в кіберпросторі, яка забезпечує сталий розвиток інформаційного суспільства, цифрового середовища, швидке виявлення та реагування на загрози безпеці. Це збереження конфіденційності та цілісності інформації у кіберпросторі. Таким чином, кібербезпека стосується захисту прав і свобод громадян в ході пересування кіберпростором та національних інтересів держави.

Кіберзахист – це система організаційних, правових, інженерно-технічних та інших заходів, спрямованих на запобігання кіберзагрозам, ліквідацію їх наслідків, відновлення надійності інформаційних систем. Деякі дослідники вважають, що ми вступили в фазу кібервійн (кіберінтревенції), оскільки факти небезпечних дій в кіберпросторі зростають кількісно та якісно.

Кіберінтервенція – це комплекс суспільно небезпечних дій, які наносять шкоду важливим сферам існування держави та суспільства. Різні сектори державного, економічного, суспільного життя стають більш уразливими до подібного роду дій, потребують захисту.

Кіберзлочинність набула характеру транснаціонального. Кібергрупи та окремі хакери активізуються, здійснюють атаки на урядові та приватні сайти, порушують роботу інформаційних ресурсів.

Поширився кардінг – фінансові злочини в кіберпросторі. Серед наслідків кіберінцидентів різного характеру завдання удару авторитету держави, розповсюдження неправдивої інформації, дезорієнтація населення, збір цінної інформації, порушення функціонування сайтів, комп'ютерних систем, об'єктів критичної інфраструктури. У 2014 році в Україні було зафіксовано 216 кібератак ззовні, більша частина я яких була здійснена на державні установи. У 2015 році кількість таких атак значно збільшилась. Кожен третій комп'ютер в Україні заражений шкідливими програмами. На одне з 36 мобільних пристроїв встановлені небезпечні додатки. Один з 13 пошукових запитів призводять до шкідливих програм. Тому одним із важливих завдань держави є встановлення таких рівнів захисту інформації, як: запобігання (надання доступу виключно персоналу), виявлення (раннє виявлення злочинних дій), обмеження (зменшення масштабів наслідків злочинів), відновлення (можливість відновлення втраченої інформації).

Створення безпечного кіберпростору передбачає впровадження системи заходів на декількох рівнях одночасно: політичному, юридичному, міжнародному, освітньому, науково-технічному. З кожним роком органи публічного управління дедалі більше залежать від технологій та переводять свою діяльність у цифровий світ. Постає проблема якісної взаємодії з громадянами, що потребує створення нового формату відносин у рамках процесу діджиталізації в Україні.

Кіберзагрози несуть реальні ризики та зумовлюють орієнтацію на цифрову грамотність в публічному управлінні. Здатність ефективно використовувати сучасні цифрові технології – важливе вміння сучасного державного службовця. В умовах децентралізації важливим є й забезпечення компетенції цифрової грамотності в органах місцевого самоврядування.

Україна має орієнтуватись на кращі зарубіжні практики зі створення ефективної системи кіберзахисту, розширювати міжнародну співпрацю в цьому напрямку. У 2005 році була ратифікована Конвенція Ради Європи про кіберзлочинність від 2001 року. Вона була створена для запобігання поширення кіберзлочинності, вказує на необхідність співробітництва між державами з метою створення більш ефективної системи захисту своїх інтересів у ході використання інформаційних технологій.

Це перша спроба у Європі об'єднати зусилля у боротьбі із кіберзлочинністю. Після підписання Україною Угоди з ЄС наша держава взяла на себе зобов'язання впроваджувати чинне законодавство Союзу, в тому числі, у сфері кібербезпеки.

Висновки. В новому середовищі, яким є кіберпростір, особливо актуальною проблемою для всіх сучасних країн є кіберзахист та кібербезпека. XXI століття є часом поширення кібератак та кіберзлочинів різного характеру.

Тому метою України зараз є посилення кіберзахисту, захист прав і свобод громадян, державних інтересів. Нашою країною були ратифіковані відповідні міжнародні угоди, створена юридична база для запуску та функціонування системи кіберзахисту. Для її вдосконалення слід розширювати міжнародну співпрацю, запозичувати корисний досвід, об'єднувати зусилля. Напрямом подальшої роботи є конкретизація Стратегії кібербезпеки України, розробка додаткових нормативно-правових актів, швидка координація дій компетентних органів. Система кіберзхисту має загальнодержавний характер, включаючи декілька напрямків: міжнародний, політичний, юридичний, організаційний, освітній.

Список використаних джерел:

1. Бакалінська О., & Бакалінський О. Правове забезпечення кібербезпеки в Україні. Піприємництво, господарство і право, 2019. 9, 100-108. https://doi.org/10.32849/2663-5313/2019.9.17

2. Грицюк Ю.І. Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання. Науковий вісник НЛТУ, 2016. 26(8), 327-337. https://doi.org/10.15421/40260850

3. Трофименко О., Прокоп Ю., Логінова Н., & Задерейко О. Кібербезпека України: аналіз сучасного стану. Захист інформації, 2019. 150-157.https://doi.org/10.18372/2410-7840.21.13951

Савчин Євгенія Андріївна
Студентка н.гр. 117 СПД ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

РОЛЬ «ШІ» У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Штучний інтелект і кібербезпека стають все важливішими в сучасному світі, де кількість кібератак постійно зростає.

Особи, які відповідають за прийняття рішень у різних сферах, зосереджують увагу на аналізі та поліпшенні кібербезпеки. Але це не просте завдання, оскільки треба забезпечити баланс між захистом особистих даних і відповідністю нормативам.